

E-FILED on 11/8/10

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE DIVISION

FORTINET, INC.,

Plaintiff,

v.

PALO ALTO NETWORKS, INC.,

Defendants.

No. C-09-00036 RMW

ORDER CONSTRUING CLAIMS OF THE  
'990 PATENT, GRANTING PAN'S MOTION  
FOR SUMMARY JUDGMENT OF NON-  
INFRINGEMENT, AND DENYING PAN'S  
MOTION FOR SUMMARY JUDGMENT OF  
INVALIDITY

[Re Docket Nos. 64, 67, 75]

Fortinet, Inc. ("Fortinet") alleges that Palo Alto Networks, Inc. ("PAN")'s firewall products infringe claims 1, 3, 5, 10 to 15, 17, 18, 32, 33, 36, 37, 40, 41, 44, and 45 of United States Patent No. 7,519,990 ("990 Patent"). The parties seek construction of claim language in the '990 Patent. PAN moves for summary judgment that the accused products do not infringe the asserted claims of the '990 Patent and that the asserted claims of the '990 Patent are invalid. The court held a tutorial and claim construction hearing on July 20, 2010. After consideration of the claims, specification, prosecution history, and other relevant evidence, and after hearing the argument of the parties, the court construes the disputed claim language in the '990 Patent as set forth below. In addition, for the

ORDER CONSTRUING CLAIMS OF THE '990 PATENT, GRANTING PAN'S MOTION FOR SUMMARY JUDGMENT OF NON-INFRINGEMENT, AND DENYING PAN'S MOTION FOR SUMMARY JUDGMENT OF INVALIDITY—No. C-09-00036 RMW CCL

1 reasons set forth below, the court grants the motion for summary judgment of non-infringement and  
2 denies the motion for summary judgment of invalidity.

### 3 I. BACKGROUND

4 This case deals with firewall technology. Firewalls control network traffic traveling between  
5 networks or zones of different trust levels, such as between the Internet and a local area network  
6 ("LAN"). Dkt. No. 146 ¶ 12. In order to protect a LAN from undesirable content, such as viruses  
7 and spam, firewalls analyze incoming and outgoing network traffic. *Id.* ¶ 15. Network traffic  
8 consists of packets of data. A data packet has seven protocol layers: the physical layer (L1), data  
9 link layer (L2), network layer (L3), transport layer (L4), session layer (L5), presentation layer (L6),  
10 and application layer (L7). *Id.* ¶ 17. TCP and UDP are common transport layer protocols. *Id.* ¶ 23.  
11 IP is an example of a network layer protocol, and Ethernet is an example of a data link layer  
12 protocol. *Id.* ¶ 21. Each layer has a header that contains information identifying the protocol of the  
13 next higher layer. *Id.* ¶ 19. Based on this header information and an inspection of the packet to see  
14 if it conforms with the required packet format for a protocol, a firewall can determine the protocols  
15 used to enclose a data packet. *See id.* ¶ 19.

16 The '990 Patent teaches a system and method for analyzing the content of computer and  
17 network traffic using two processors. The first processor receives network content and determines  
18 whether the protocol of the network traffic matches a prescribed protocol that may contain content  
19 sought to be detected. If there is not a match, the first processor filters the network content itself. If  
20 the protocol matches the prescribed protocol, the first processor stores the network content in a stack  
21 for content inspection by the second processor. The second processor then determines whether the  
22 network traffic content stored in the stack contains content sought to be detected. For illustrative  
23 purposes, claim 1 of the '990 Patent is set forth below:

24 A device for managing network traffic flow, the device comprising:  
25 a first processor, the first processor configured to  
26 receive network traffic content,  
27 determine whether a protocol of the network traffic content matches a  
28 prescribed protocol of network traffic content that could contain content  
desired to be detected by comparing a type of the network traffic content  
with a prescribed type,  
store the network traffic content in a stack when the protocol of the  
network traffic content matches the prescribed protocol, and

perform filtering of the network traffic if the type of the network traffic content does not match the prescribed type; and a second processor associated with the stack, wherein the second processor is configured to determine whether the network traffic content contains the content desired to be detected if the type of the network traffic content matches the prescribed type.

'990 Patent 23:24-43.

The accused products are PAN's PA-4000 Series, PA-2000 Series, and PA-500 Series Firewalls. [REDACTED]

## II. CLAIM CONSTRUCTION

The parties agree that a "stack" refers to memory for temporary storage. They seek construction of the terms in bold in the following claim language:

determine<sup>1</sup> whether a protocol of the network traffic matches a **prescribed protocol of network traffic content that could contain content desired to be detected** by comparing a type of the network traffic content with a prescribed type, . . .

store<sup>2</sup> the network traffic content in a stack when the protocol of the network traffic content matches **the prescribed protocol** . . . .

'990 Patent 23:27-35 (claim 1), 24:17-27 (claim 15). Their proposed constructions for the disputed claim terms are set forth below:

CLAIM LANGUAGE	FORTINET'S PROPOSED CONSTRUCTION	PAN'S PROPOSED CONSTRUCTION
"a prescribed protocol of network traffic content that could contain content desired to be detected"	A recognized protocol of network traffic content that could contain content desired to be detected.	Any protocol that has been pre-identified as potentially containing content desired to be detected.

<sup>1</sup> "Determining" in claim 15.

<sup>2</sup> "Storing" in claim 15.

CLAIM LANGUAGE	FORTINET'S PROPOSED CONSTRUCTION	PAN'S PROPOSED CONSTRUCTION
"the prescribed protocol"	A recognized protocol.	One of the set of protocols that have been pre-identified as potentially containing content desired to be detected.

It is undisputed that to "prescribe" means to set down as a rule. Thus, a prescribed protocol is a protocol that has been set down by rule. The court declines to construe "prescribed" as recognized or pre-identified because such a construction would be over-inclusive. Although a prescribed protocol has necessarily been recognized and pre-identified, not all recognized or pre-identified protocols need be prescribed.

It appears that the real dispute is not whether "prescribed" means recognized or pre-identified. Rather, the heart of the dispute lies in whether "prescribed," as used in the '990 Patent, refers to having set down a rule regarding a protocol *because the protocol could contain content desired to be detected*, as PAN contends, or more broadly refers to having set down a rule regarding a protocol, regardless of the reason for the rule, as argued by Fortinet. In other words, PAN construes "a prescribed protocol of network traffic content that could contain content desired to be detected" as meaning a protocol of network traffic content that is prescribed *because* it could contain content desired to be detected. Fortinet, on the other hand, construes the claim language to mean a protocol of network traffic content that is prescribed *and* that could contain content desired to be detected. The court agrees with Fortinet's construction.

Since to "prescribe" simply means to set down as a rule, there is nothing in the claim language to suggest that the claims require a protocol to be set down by rule because it could contain content desired to be detected. Furthermore, the specification, which is the "single best guide to the meaning of the disputed term," *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005), confirms that a prescribed protocol need not be a protocol set down by rule because it could contain content desired to be detected. In supporting its proposed construction, PAN quotes from a portion of the specification, which states, "In the illustrated embodiments, protocol differentiator 704 is configured to pass safe traffic content to packet processing module 706, and unsafe traffic content to

1 stack 708." '990 Patent 8:48-51. This statement, standing alone, might suggest that the only  
2 contemplated reason for setting down a rule regarding a protocol would be because it could contain  
3 content desired to be detected. However, immediately following this statement, the specification  
4 goes on to explain:

5 In alternative embodiments, protocol differentiator 704 is configured to pass  
6 potentially undesirable network traffic content to both packet processing module 706  
7 and stack 708. In such case, network traffic content that can be screened by  
8 conventional content filtering techniques may be passed to packet processing module  
9 706, while other traffic content, such as those that may contain virus or worms, may  
10 be passed to stack 708. In some embodiments of the invention, processor 702 may be  
11 programmable or configurable such that a user can prescribe certain types of network  
12 traffic content to be passed to packet processing module 706 or to stack 708.

13 '990 Patent 8: 51-62. By disclosing embodiments of the invention where rules regarding network  
14 traffic are based on whether the traffic can be screened by conventional techniques, rather than  
15 based on whether the traffic may contain potentially undesirable content, the specification makes  
16 clear that a protocol may be set down by rule for reasons other than the fact that it could contain  
17 content desired to be detected. The fact that users may program or configure the processor to set  
18 their own rules for prescribing network traffic content further bolsters Fortinet's argument that a  
19 protocol may be set down by rule for any number of reasons. Accordingly, the court finds that "a  
20 prescribed protocol of network traffic content that could contain content desired to be detected" is a  
21 protocol of network traffic content that has been set down by rule and that could contain content  
22 desired to be detected.

23 As for the second disputed claim term in the '990 Patent, "the prescribed protocol" does not  
24 refer generally to any prescribed protocol. In the context of the claims, it is clear that "the  
25 prescribed protocol" refers specifically to the earlier claim language describing "a prescribed  
26 protocol of network traffic content that could contain content desired to be detected." *See, e.g.,* '990  
27 Patent 23:27-35. Hence, the court construes "the prescribed protocol" as the protocol of network  
28 traffic content that has been set down by rule and that could contain content desired to be detected.

### III. NON-INFRINGEMENT

Each of the asserted claims in the '990 Patent requires the use of two processors, with the  
first processor comparing a protocol of the network traffic content with a prescribed protocol to

1 determine whether there is a match and, based on this determination, either forwarding the network  
2 traffic content to a second processor for content inspection or performing filtering of the network  
3 traffic on its own. *See* '990 Patent 23:24-26:45.

4 [REDACTED]  
5 [REDACTED] Fortinet has set forth two theories of infringement.  
6 Under one theory, the prescribed protocols are TCP or UDP, which are transport layer protocols.  
7 Under another theory, the prescribed protocol is IP, a network layer protocol. The court considers  
8 each theory of infringement.

9 **A. TCP or UDP as the Prescribed Protocol**

10 The asserted claims require comparing a protocol of the network traffic content with a  
11 prescribed protocol to determine whether there is a match.<sup>3</sup> '990 Patent 23:27-31, 24:17-21. Fortinet  
12 contends that the accused products meet this limitation because [REDACTED]  
13 [REDACTED]

14 PAN argues that the accused products fail to meet this limitation because "malformed TCP or UDP  
15 packets" lack a legitimate protocol and therefore cannot be compared against a prescribed protocol  
16 to determine whether there is a match.

17 A data packet has seven protocol layers: the physical layer (L1), data link layer (L2),  
18 network layer (L3), transport layer (L4), session layer (L5), presentation layer (L6), and application  
19 layer (L7). Dkt. No. 146 ¶ 17. Each layer has a header that contains information identifying the  
20 protocol of the next higher layer. *Id.* ¶ 19. However, packets are sometimes malformed, which can  
21 occur because part of a packet is not transmitted or part of a header has been changed. *See id.* Such  
22 malformed packets are discarded because the information in the packet cannot be used. *See id.*  
23 In determining what protocols have been used to enclose a data packet, firewalls not only look at  
24 header information but also inspect the packet to see if it conforms with the required packet format  
25 for a particular protocol. *See id.* Thus, a packet that initially appears to be of the TCP or UDP

26  
27 <sup>3</sup> The claims require "determining whether a protocol of the network traffic content matches with a  
28 prescribed protocol of network traffic content . . . by comparing a type of the network traffic content  
with a prescribed type." '990 Patent 24:17-21. The parties agree that "type," as used in the '990  
Patent, means "protocol" because the two words are used interchangeably throughout the patent.



1 protocol based on header information may actually fail to conform to the required packet format for  
2 the TCP or UDP protocol and thus be discarded. Fortinet refers to these as "malformed TCP or UDP  
3 packets." These so-called "malformed TCP or UDP packets" are not legitimate packets of the TCP  
4 or UDP protocol. *See id.*

5 [REDACTED]  
6 [REDACTED] *See* Dkt.  
7 No. 144 ("Zuk Dep.") 166:25-168:7. Because these packets are malformed, they lack a transport  
8 layer protocol. *See* Dkt. No. 146 ¶ 19. After all, by definition, a "malformed TCP or UDP packet"  
9 fails to conform to the required packet format for the TCP or UDP protocol. [REDACTED]  
10 [REDACTED]

11 [REDACTED] Therefore, the  
12 accused products do not compare a protocol of the network traffic content with a prescribed protocol  
13 to determine whether there is a match and thus do not infringe any of the asserted claims under this  
14 theory of infringement.

#### 15 **B. IP as the Prescribed Protocol**

16 Under Fortinet's other theory of infringement, IP Ethernet packets match the prescribed  
17 protocol, while non-IP Ethernet packets do not match the prescribed protocol. PAN argues that the  
18 accused products do not infringe the '990 Patent under this theory because [REDACTED]  
19 [REDACTED]

20 The asserted claims require the first processor to "perform filtering of the network traffic if  
21 the type of the network traffic content does not match the prescribed type." '990 Patent 23:35-37.  
22 "Filtering" was not one of the terms initially chosen for claim construction. However, because the  
23 meaning of "filtering," as used in the '990 Patent, is central to the parties' dispute over non-  
24 infringement, the court permitted the parties to submit supplemental briefing on this issue. The  
25 supplemental briefing made clear that, although the parties disagree regarding the scope of actions  
26 that could constitute "filtering,"<sup>4</sup> they agree that "filtering" means to separate data, signals, or

27  
28 <sup>4</sup> PAN argues that "filtering" is limited to allowing or blocking content, while Fortinet contends that  
"filtering" includes allowing, blocking, or modifying content.

1 material in accordance with specified criteria. *See* Dkt. No. 191 at 5. In other words, "filtering"  
 2 requires treating different kinds of content differently based on some specified criteria and does not  
 3 include treating all content the same way. Because this agreed understanding of "filtering" is  
 4 dispositive on the question of non-infringement, the court need not address the finer points of  
 5 disagreement and simply adopts this agreed-upon definition.

6 [REDACTED]  
 7 [REDACTED]  
 8 [REDACTED]  
 9 [REDACTED]  
 10 [REDACTED]  
 11 [REDACTED]  
 12 [REDACTED]  
 13 [REDACTED]  
 14 [REDACTED]  
 15 [REDACTED]  
 16 [REDACTED]  
 17 [REDACTED]  
 18 [REDACTED]  
 19 [REDACTED]  
 20 [REDACTED]  
 21 [REDACTED]  
 22 [REDACTED] the accused products also do not infringe any of the asserted claims under this theory of  
 23 infringement.<sup>5</sup>

24  
 25  
 26  
 27 <sup>5</sup> In opposing PAN's motion for summary judgment, Fortinet did not argue that the accused products  
 28 infringed under the doctrine of equivalents. Neither its original infringement contentions, nor the  
 proposed amendments, adequately assert the doctrine of equivalents.



**C. PA-500 Series Firewall**

None of the accused products infringe the asserted claims of the '990 Patent for the reasons explained above. The PA-500 Series Firewall does not infringe for an additional reason: it does not meet the two processor limitation. [REDACTED]

[REDACTED] See Zuk Dep. 41:14-21. However, this is insufficient to meet the requirements of the '990 Patent because the second processor must be configured to "determine whether the network traffic content contains the content desired to be detected." '990 Patent 23:39-41, 24:28-30. [REDACTED]

[REDACTED] See Zuk Dep. 40:12-41:12. Therefore, the PA-500 Series Firewall does not infringe the asserted claims of the '990 Patent for this additional reason.

**IV. INVALIDITY**

PAN seeks summary judgment that the asserted claims of the '990 Patent are invalid as anticipated by the Nortel Alteon Switched Firewall ("Nortel ASF"). The Nortel ASF is a firewall that consists of a Firewall Accelerator and a Firewall Director. See Dkt. No. 68 Ex. A at 17. PAN alleges that the Nortel ASF contains each and every limitation of the asserted claims of the '990 Patent in the following manner: The Accelerator is the first processor, and the Director is the second processor. The Accelerator receives network traffic content, determines the protocol of that network traffic, and applies a set of rules to determine what to do with the network traffic content based on the protocol of the network traffic. See Dkt. No. 65 ¶¶ 38-39. Based on those rules, if the protocol of the network traffic is prescribed, the Accelerator uses a fiber optic Ethernet connection to store the network traffic content in memory at the Director. See *id.* ¶ 55. If the protocol of the network

1 traffic is not prescribed, the Accelerator instead filters the network traffic itself. *See* Dkt. No. 68 Ex.  
2 A at 145, 149. According to PAN, the Director inspects network traffic content received from the  
3 Accelerator to determine whether it contains undesirable content. *See* Dkt. No. 65 ¶ 58.

4 Fortinet argues that the asserted claims of the '990 Patent are not anticipated by the Nortel  
5 ASF because: (1) the Nortel ASF does not qualify as prior art, and (2) the Firewall Director (the  
6 alleged second processor in the Nortel ASF) does not perform content inspection.

#### 7 A. Prior Art

8 The '990 Patent claims priority to July 19, 2002, the filing date of its earliest provisional  
9 application. Fortinet does not claim that the invention was conceived and reduced to practice any  
10 earlier than this date. PAN contends that the Nortel ASF qualifies as prior art because it had been  
11 used prior to July 19, 2002.

12 35 U.S.C. § 102(a) provides that "[a] person shall be entitled to a patent unless – (a) the  
13 invention was known or used by others in this country . . . before the invention thereof by the  
14 applicant for the patent." In order for the prior use to invalidate a patent, the use must be "accessible  
15 to the public." *Woodland Trust v. Flowertree Nursery, Inc.*, 148 F.3d 1368, 1370 (Fed. Cir. 1998).  
16 "[A]ny use of the claimed invention by a person other than the inventor who is under no limitation,  
17 restriction, or obligation of secrecy to the inventor" qualifies as a use that is accessible to the public.  
18 *New Railhead Mfg., L.L.C. v. Vermeer Mfg. Co.*, 298 F.3d 1290, 1297 (Fed. Cir. 2002).

19 It is undisputed that the Nortel ASF was a commercial product sold by Nortel in late 2001  
20 and that Dr. Lavian bought this product in early 2002 and gave a presentation about it in May 2002.  
21 *See* Dkt. No. 65 ¶ 30; Dkt. No. 109 Ex. C ("Lavian Dep.") 54:14-19. Because Dr. Lavian used the  
22 Nortel ASF in a laboratory setting, *see* Dkt. No. 65 ¶ 24, Fortinet argues that Dr. Lavian's use of the  
23 Nortel ASF was experimental. However, "[e]xperimental use, which means perfecting or  
24 completing an invention to the point of determining that it will work for its intended purpose, ends  
25 with an actual reduction to practice." *RCA Corp. v. Data General Corp.*, 887 F.2d 1056, 1061 (Fed.  
26 Cir. 1989). Accordingly, "experimental use cannot negate a public use when it is shown that the  
27 invention was reduced to practice before the experimental use." *In re Omeprazole Patent Litig.*, 536  
28 F.3d 1361, 1372 (Fed. Cir. 2008). As a commercial product, the Nortel ASF had clearly been

1 reduced to practice by the time Dr. Lavian purchased it. Thus, Dr. Lavian's use of the Nortel ASF  
2 was not an experimental use and constitutes a use that is accessible to the public. Since this use  
3 occurred prior to the claimed invention date of July 19, 2002, the Nortel ASF qualifies as prior art  
4 under 35 U.S.C. § 102(a).

5 **B. Content Inspection**

6 The '990 Patent requires that the second processor be "configured to determine whether the  
7 network traffic content contains the content desired to be detected if the type of the network traffic  
8 content matches the prescribed type." '990 Patent 23:39-43, 24:28-31. The parties agree that in  
9 order for the Nortel ASF to meet this limitation, the Director (the second processor) must inspect  
10 network traffic received from the Accelerator (the first processor). According to PAN, Security  
11 Servers, which are software entities on the Director, perform content inspection by running Check  
12 Point Firewall-1 software to determine whether network traffic contains undesirable content.  
13 Fortinet argues that the Security Servers on the Director do not actually perform content inspection  
14 themselves but rather pass network traffic on to third party servers on another processor for content  
15 inspection.

16 It is undisputed that some content inspection, such as anti-virus screening, may be offloaded  
17 to a Content Vectoring Server, which exists on a separate processor, not on the Director. There is a  
18 factual dispute, however, as to whether the Security Servers on the Director ever perform any  
19 content inspection on their own. Having reviewed the evidence in the record, the court concludes  
20 that this dispute raises a genuine issue of material fact.

21 Various Check Point documents state that the Security Servers on the Director implement  
22 content security or are used to provide content security. *See, e.g.*, Dkt. No. 65 Ex. J at PAN 008903  
23 ("FireWall-1 provides content security for HTTP, SMTP, and FTP connections using the FireWall-1  
24 Security Servers."); Dkt. No. 109 Ex. D at 12 ("Content security is defined using Resource objects  
25 and implemented by the Security Servers."). However, these statements fail to clarify whether the  
26 Security Servers actually perform the content inspection themselves or simply "implement content  
27 security" by passing network traffic on to third party servers for content inspection. The "Check  
28 Point FireWall-1 Technical Overview" provides some explanation of the role that Security Servers

1 play in its description of how a Resource object (which defines the prescribed protocol) works in  
2 conjunction with Security Servers:

3 A Resource object defines a group of entities accessed by a specific protocol. . . .  
4 When a connection matches a rule with a Resource, the FireWall-1 Inspection  
Module diverts the connection to the appropriate Security Server.

5 *The Security Server can then query a third-party server, such as a URL filtering*  
6 *server, which performs the required content inspection.* FireWall-1 processes the  
original connection depending on the reply from the server and the action in the rule.

7 Dkt. No. 109 Ex. D at 12 (emphasis added). While this explanation does not conclusively preclude  
8 the possibility that Security Servers sometimes perform content inspection on their own, it suggests  
9 that the role Security Servers play in implementing content security is to query third-party servers,  
10 which actually perform the content inspection.

11 PAN points to the following statement in a Check Point press release as evidence that the  
12 Security Servers on the Director do not always rely on third party servers to conduct content  
13 inspection: "Check Point FireWall-1 3.0's content security features are comprised of the Content  
14 Vectoring Protocol (CVP), an open protocol for integrating external and third-party content  
15 inspection programs, *plus integrated content inspection capabilities for anti-virus protection, URL*  
16 *screening, and Java security.*" Dkt. No. 109 Ex. E at 1-2 (emphasis added). It remains unclear,  
17 however, whether the "integrated content inspection capabilities" occur on the Security Servers on  
18 the Director. Another Check Point document states that URL screening occurs "using third party  
19 URL Filtering Protocol (UFP) servers." Dkt. No. 109 Ex. D at 13. Thus, at least one such  
20 "integrated" capability appears to rely on third party servers for content inspection.

21 The Check Point documents in the record do not conclusively rule out the possibility that  
22 Security Servers may perform some type of content inspection on their own. In fact, one technical  
23 document suggests that some Java security may be implemented without third party servers since it  
24 lists various Java security capabilities followed by the statement that "FireWall-1 *also* integrates  
25 Java screening capabilities of third-party applications." *Id.* at 13. However, "[p]atents enjoy a  
26 presumption of validity, 35 U.S.C. § 282 (2006), and a party seeking to invalidate a patent must  
27 overcome this presumption by facts supported by clear and convincing evidence." *Iovate Health*  
28 *Sciences, Inc. v. Bio-Engineered Supplements & Nutrition, Inc.*, 586 F.3d 1376, 1380 (Fed. Cir.

2009). PAN has not met its burden of establishing that the Director performs content inspection by clear and convincing evidence. The court therefore denies its motion for summary judgment of invalidity.

### V. ORDER


For the foregoing reasons, the court:

1. Construes the claim language as set forth below:

CLAIM LANGUAGE	CONSTRUCTION
"stack"	Memory of temporary storage.
"a prescribed protocol of network traffic content that could contain content desired to be detected"	A protocol that has been set down by rule and that could contain content desired to be detected.
"the prescribed protocol"	The protocol that has been set down by rule and that could contain content desired to be detected.
"filtering"	Separating data, signals, or material in accordance with specified criteria.

2. Grants PAN's motion for summary adjudication that the accused products do not infringe the asserted claims of the '990 Patent; and
3. Denies PAN's motion for summary adjudication that the '990 Patent is invalid.

DATED: 11/8/10

  
 RONALD M. WHYTE  
 United States District Judge